

## Cloud Workload Protection Features in Different Editions Product Documentation



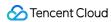


## Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.



## Features in Different Editions

Last updated : 2020-04-10 09:59:26

Pro edition is coming soon.

Main features in different CWP editions are compared in the table below:

| Feature and Description                                                                                                                    | Basic                                                                                                    | Pro       |
|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|-----------|
| Web shell detection  Detects common web script trojans and backdoors, covering various script languages such as ASP, PHP, JSP, and Python. | CWP Basic can detect at most 5 web shells free of charge and stops detection after the limit is reached. | Supported |
| Hacker tool detection  Detects common hacking and attacking programs such as DDoS trojans, remote controllers, and cryptomining malware.   |                                                                                                          | Supported |
| <b>Binary virus and trojan detection</b> Detects detect binary executable viruses and trojans such as .exe, .ddl, and .bin files.          |                                                                                                          | Supported |
| Password cracking attack detection Alerts users on common password cracking attacks by hackers.                                            | Supported                                                                                                | Supported |
| <b>Login transaction audit</b> Analyzes login logs on the server to detect malicious logins.                                               | Supported                                                                                                | Supported |
| Risky configuration item detection Inspects certain system component configuration items to prevent vulnerabilities.                       | -                                                                                                        | Supported |
| Weak account password detection Checks for weak passwords in system accounts.                                                              | CWP Basic can detect at most 5 issues and stops detection after the limit is reached.                    | Supported |
| Web component vulnerability                                                                                                                |                                                                                                          | Supported |



| <b>detection</b> Provides vulnerability detection in common web components such as phpMyAdmin and WordPress.                                            |   |       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|---|-------|
| Common component vulnerability detection Provides vulnerability detection in common components such as Apache, Nginx, Struts, and Redis.                |   | Suppo |
| <b>System-level vulnerability detection</b> Detects system-level vulnerabilities (mainly those can be fixed by OS patches).                             |   | Suppo |
| <b>Vulnerability repair solution push</b> Provides repair and prevention solutions for detected vulnerabilities.                                        |   | Suppo |
| <b>0-day vulnerability intelligence push</b> Pushes the latest vulnerability intelligence based on the vulnerability intelligence collected by Tencent. | - | Suppo |
| Expert service Provides an 8/5 expert support hotline. You can submit a ticket to request a callback.                                                   | - | Suppo |